Department of Electrical Engineering
香港城市大學
City University of Hong Kong

CityU Architecture Lab for Arithmetic and Security (CALAS) Seminar Series

GPU Acceleration for Word-Wise Homomorphic Encryption

Dr. Hao YANG, PhD Scholar

Nanjing University of Aeronautics and Astronautics

Abstract:

(Fully) Homomorphic Encryption (HE) is a promising privacy-enhancing cryptographic technique that allows computations to be performed on encrypted data without the need for decryption, and it has potentially wide applications across various industries. However, the primary challenge faced by HE is its low performance. The GPU, a powerful accelerator not only for AI tasks but also for cryptographic computations, is explored to accelerate HE in this context. This presentation first provides a brief overview of HE and its applications, then delves into the implementation details of HE. We explore several optimizations for both low-level arithmetic and high-level homomorphic operations on GPUs. Building on these foundations, we introduce an open-sourced GPU library specifically for word-wise HE schemes, named PhantomFHE. Finally, some potential directions for future research are discussed.

Biography:

Hao YANG completed his bachelor's and PhD degrees from Nanjing University of Aeronautics and Astronautics in 2019 and 2024, respectively. His research focuses on lattice-based cryptography, fully homomorphic encryption, and GPU acceleration. He has published in journals including IEEE TIFS, IEEE TDSC, and IEEE TC. He has participated in more than 5 national projects from NSFC and MOST. He has also participated as a main contributor in projects funded by Ant Group and Huawei.

3 May 2024 (Fri); 10:00am - 12:00nn; P1402; https://cityu.zoom.us/j/96742093029